Defending against distributed denial of service (DDoS) attacks – ITSM.80.110

From: Canadian Centre for Cyber Security

February 2024 **Management series** **ITSM.80.110**

Foreword

This is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre).
For more information, email, or phone our Contact Centre:

✉ contact@cyber.gc.ca | 📱 613-949-7048 or 1-833-CYBER-88

Alternate format: Defending against distributed denial of service (DDoS) attacks - ITSM.80.110 (PDF, 468 Kb)

Effective date

This publication takes effect on February 20, 2024.

Revision history

1. **First release:** February 20, 2024.

▸ Table of Contents

Overview

As technology evolves, distributed denial of service (DDoS) attacks are becoming more sophisticated and widespread. These attacks, commonly used by cybercriminals, can cause significant financial, operational, and reputational damage to organizations worldwide. Regardless of the type of DDoS attack, the main goal is always to overwhelm and incapacitate targeted servers, services, or networks by flooding them with malicious traffic from compromised devices or networks.

To effectively defend against these threats, it's crucial to implement a defence strategy that will enhance your organization's resilience to DDoS attacks. Implementing scalable and resilient multilayered DDoS protection solutions is a vital part of this defence strategy. For organizations with limited cyber security resources, engaging with a managed service provider (MSP) is a recommended option. MSPs specializing in cyber security bring expertise, advanced technologies, and 24/7 monitoring for early threat detection. They respond swiftly to mitigate attacks and adjust services based on network needs.

The main objective of this publication is to help your organization reduce the likelihood of DDoS attacks, to minimize the impact should an attack occur, and to enhance your overall defence solution by implementing mitigation strategies and leveraging lessons learned from past DDoS attacks.

The mitigation strategies identified in this publication can also improve your organization's overall security posture and resilience and assist in defending against other types of threats or attacks.

1 Introduction

In the ever-growing landscape of cyber security, distributed denial of service (DDoS) attacks continue to pose a persistent and growing threat. The National Cyber Threat Assessment 2023-2024 [1] describes DDoS attacks as an evolving method of extortion used by threat actors to compromise Canadian organizations of all sizes. These attacks, carried out by individuals or groups with malicious intent, have the potential to disrupt and cripple online services, wreaking havoc on organizations and even entire industries.

This publication details the various types of DDoS attacks, the motivations behind them, the methods used by threat actors, and, most importantly, the mitigation strategies your organization can use to improve your defences and protect your online presence. To safeguard your digital infrastructure, the essential first step is understanding what a DDoS attack entails.

Top of page

1.1 What is a DDoS attack?

DDoS is a cyber attack that directs a large volume of malicious Internet traffic at a target, often a website or any Internet-connected service, aiming to overwhelm and disable it. Threat actors, including individual hackers, criminal groups, and foreign state actors, execute these attacks to disrupt normal network, service, or website operations, DDoS attacks cause poor performance or a complete shutdown.

While a DDoS attack can be a coordinated effort between a group of threat actors, it can also be carried out by one person using a botnet, which are large networks of computers that have been compromised or infiltrated by a threat actor to send a massive amount of traffic to the target to disrupt access for legitimate users or systems. They can persist for an extended period, lasting from days or even weeks, inflicting harm to organizations and businesses.

Top of page

1.2 Potential impacts on your organization

DDoS attacks can have harmful consequences for your organization, including:

- **Financial setbacks:** A successful DDoS attack can lead to reduced productivity, downtime, loss of revenue, and significant costs to mitigate and recover from the attack.
- **Operational disruption:** DDoS attacks can cripple your organization's core operations or hinder customers' access to services.
- **Damage to reputation:** DDoS attacks can potentially undermine trust and loyalty among customers, compelling them to choose competitors due to their inability to access the desired website or by seeding doubts about its reliability.
- **Increased system security risks:** DDoS attacks can reveal existing weaknesses in a corporate network which may then be leveraged by threat actors to carry out additional attacks or gain unauthorized access to the system.

1.3 Difference between DoS and DDoS

While DDoS and denial of service (DoS) attacks share similar names and objectives of disrupting network, service, or website availability, they differ primarily in scale and execution.

A DoS attack is carried out by a single source or threat actor, aiming to exploit software vulnerabilities or overwhelm a system or process by sending a large amount of data or requests to the target. Like a DDoS attack, the goal is to overwhelm the target to the extent that it becomes incapable of handling legitimate user requests. This can cause delays, service disruptions, or complete shutdown of the targeted systems or network. For more information on a DoS attack and its impact on your organization, you can refer to the publication Protecting your organization against denial of service attacks [2].

Contrary to a DoS attack, a DDoS attack is more sophisticated and involves multiple connected devices working in tandem to overwhelm the target. The collective power of this compromised network of devices makes it challenging to defend against because it can overwhelm even the most robust network infrastructure and security measures. Not only does a DDoS attack increase the attack power, it also makes it harder to identify the true source of the attack.

2 Common types of DDoS attacks

While the end goal of a DDoS attack is to make an online service unavailable to users, the methods employed to execute the goal can vary. The different types of DDoS attacks target different parts of a network and are categorized based on the network connection layers they exploit. The three broad types are: volumetric attack, protocol attack, and application layer attack.

2.1 Volumetric attacks

The most common type of DDoS attack is a volumetric attack. This type of attack focuses on overwhelming the network with false data requests and exhausting the network bandwidth and processing capabilities, resulting in denial of service for legitimate users. This is often accomplished by using botnets. An example of a volumetric attack is domain name system (DNS) amplification, which uses open DNS servers to send many DNS query requests to the target, causing a traffic overload. A user datagram protocol (UDP) flood attack is another type of volumetric DDoS attack, and the goal is to flood a specific server with internet protocol (IP) packets using UDP. Because the server cannot determine the destination or intended application for these packets, it responds with "destination unreachable" messages. This flood of UDP traffic can overwhelm the server, leading to service interruptions or downtime.

2.2 Protocol attacks

Protocol attacks are a type of DDoS attack aimed at disrupting a service by exploiting vulnerabilities in the protocols used for data transfer. The goal is to overwhelm server resources and/or the resources of network equipment, such as firewalls and load balancers. Fortunately, this type of attack usually has a clear trail and can easily be detected.

An example of a protocol attack is the synchronize (SYN) flood attack, where the threat actor sends an excessive number of transmission control protocol (TCP) connection requests to the target, using spoofed source IP addresses. The targeted servers attempt to complete these connection requests, but instead of successful connections, the target becomes flooded with a large volume of connection requests. This flood of requests exhausts the target's resources, effectively tying up the system and preventing it from accepting legitimate connections.

2.3 Application layer attacks

Application layer attacks target weaknesses in an application. These attacks focus primarily on direct web traffic and can be hard to detect because a machine may struggle to distinguish them from normal, high volume internet traffic.

A common form of application layer attack is a hypertext transfer protocol (HTTP) flood, which resembles repeatedly refreshing a web browser on numerous computers simultaneously. This excessive number of HTTP requests overwhelms the server, resulting in a denial of service.

An example of an HTTP flood is Slowloris, which primarily targets web servers. In a Slowloris attack, the threat actor sends HTTP requests to a web server but never actually completes the requests. Periodically and slowly, the threat actor adds additional headers to keep the request going without ever completing it. This strategy compels the web server to maintain open connections for these partially completed HTTP requests, eventually preventing it from accepting any new connections.

Another example of an application layer attack is structured query language (SQL) injection. With this form of SQL injection, threat actors manipulate input fields on a website to execute malicious SQL queries to the database that will consume the power of the web server and the database and exhaust the server resources.

3 DDoS attack motivations

DDoS attacks can be initiated by individuals, businesses, and even nation states, each driven by their own motivations. Here are some possible motivations behind DDoS attacks:

1. **Hacktivism**: Hacktivists use DDoS attacks as a method to both protest and bring awareness to their social or political concerns. Their targets can range from governments, politicians, and large business organizations.
2. **Extortion**: Extortion has become a popular motivation for DDoS attacks, where threat actors demand ransom payments from their victims to stop a DDoS attack.
3. **Ideological reasons**: Some threat actors may initiate DDoS attacks that are driven by their ideological beliefs. This may include individuals who seek to disrupt and cause harm to companies or organizations that they view as unethical.
4. **Cyberwarfare**: Cyberwarfare is typically associated with nation states who are using state-sponsored DDoS attacks for political and military advantages. They aim to disrupt vital financial, health, and infrastructure systems within targeted countries. These strategies involve well-trained technology experts and are associated with government militaries or terrorist organizations. Many governments worldwide have invested significant resources to execute attacks that disrupt the online and critical infrastructure of their adversaries.
5. **Business competition**: DDoS attacks are increasingly being used as a strategic tool for competitive businesses. The primary objective of employing such tactics is to inflict financial and reputational damage on rival businesses, with the aim of disrupting their services to gain a competitive edge in the market. These attacks can take various forms, ranging from preventing a competitor's participation in online events to entirely disrupting their online operations for extended periods.
6. **Revenge**: Some individuals or groups who harbour frustration due to perceived injustice may launch DDoS attacks as retaliation against a person or organization.

4 How to detect a DDoS attack?

Detecting a DDoS attack involves recognizing signs that could suggest that your network is under attack. The following could potentially indicate a DDoS attack:

- **Sudden and unexpected surge in web traffic from a specific location or IP address**
  - In most cases, these connection requests are unable to be completed as the true source of IP packets are hidden.
- **Slow or irregular network performance, such as delayed website loading times**
  - This occurs when the threat actor overwhelms the server with an excessive volume of requests, leading to a noticeable system slowdown.
- **Unexplained server error messages, timeouts, or the inability to access your website**
  - This occurs when a threat actor floods your server with so many requests, causing it to become overwhelmed and resulting in a 503 "Service Unavailable" error, typically associated with service disruptions. This usually resolves itself as incoming traffic decreases. However, if the problem persists, it may suggest a more serious issue like a DDoS attack.
- **Employees complain of slow connectivity**
  - This is particularly pertinent if they share the same network connection as your website. In such a scenario, it suggests that the network's performance may be compromised and could be linked to a DDoS attack.
- **Reduced performance across other services sharing the same network**
  - This is often a result of the threat actor's requests overwhelming the network's available bandwidth, leading to slowdowns or disruptions in other services.
- **Notification from Internet service provider (ISP), cloud service provider (CSP), or other service provider**

5 Mitigation strategies for DDoS attacks

The primary challenge in mitigating a DDoS attack is distinguishing between legitimate traffic and malicious traffic. The challenge stems from the many different types of DDoS attacks on the internet. These attacks can take on various forms, ranging from simple source attacks to complex multiple source attacks.

Sophisticated DDoS attacks can leverage multiple pathways to overwhelm a target, while using different methods to divert mitigation efforts across these various routes. An example involves simultaneously targeting multiple layers of the protocol stack, such as combining a DNS amplification attack with an HTTP flood. In general, the more complex the attack, the harder it becomes to differentiate the attack traffic from legitimate traffic.

Threat actors aim to remain unnoticed so they can hinder mitigation efforts. To effectively counter these complex DDoS attacks, you should implement a multilayered defence solution to address the diverse attack routes. Your solution should be designed for scalability, with integrated redundancies, and with the ability to monitor traffic, and manage vulnerabilities effectively. In addition to the DDoS defence strategies described below, you can reference the Cybersecurity and Infrastructure Security Agency's (CISA) DDoS Quick Guide (PDF) [3] for guidance on mitigation strategies for different attack methods.

5.1 Educate your employees

Educating your employees is an important part of the overall cyber security strategy. A DDoS botnet is a tactic employed by threat actors to compromise a network of devices by remotely manipulating them to inundate a target with an overwhelming volume of traffic. Threat actors may exploit the devices of unsuspecting employees as part of this botnet. It is crucial to educate your employees, so they understand how to protect their devices from such exploitation.

Employees can significantly reduce their risk of becoming a participant in a botnet by adhering to the following precautionary steps and implementing the recommendations detailed in the applicable guidance documents noted below.

- Ensure that your devices and software are regularly updated: How updates secure your device (ITSAP.10.096) [4]
- Use multifactor authentication to protect your accounts: Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) [5]
- Be vigilant of suspicious emails and their attachments: Spotting malicious email messages (ITSAP.00.100) [6]
- Employ a trusted anti-malware solution to protect your devices: Protect your organization from malware (ITSAP.00.057) [7]
- Use a reputable virtual private network (VPN): Virtual private networks (ITSAP.80.101) [8]
- Backup your devices and information: Tips for backing up your information (ITSAP.40.002) [9]

5.2 Implement blackhole routing

Blackholing is a countermeasure to mitigate a DDoS attack by discarding incoming traffic that is targeted towards a specific IP address. With the assistance of your ISP, your network administrator can establish a blackhole route, which directs all network traffic to a null route. However, if blackhole filtering lacks specific restriction criteria, it can route both legitimate and malicious network traffic into the blackhole, permanently removing them from the network. DDoS blackhole routing is far from ideal, as it essentially accomplishes the threat actor's intended goal, which is to make the network inaccessible and potentially cause business losses. Consequently, it should be considered a last resort when alternative mitigation techniques prove ineffective. Despite its potential to help the threat actor in achieving its objectives, blackhole routing can still serve a valuable purpose when the target of the attack is a smaller site within a larger network. In such situations, the redirection of traffic away from the targeted site through blackholing can effectively shield the larger network from the adverse effects of the attack.

5.3 Implement rate limiting

Rate limiting is another technique to mitigating DDoS attacks that involves implementing restrictions on the number of requests a server can accept a specific IP address within a specific time frame. This will limit network traffic and help prevent threat actors from overwhelming system resources. Implementing rate limiting is a good way to ensure that legitimate users can still access the system resources, without hindering the overall performance of the application. While this approach alone may not provide complete protection against advanced DDoS attacks, it can serve as a valuable component to a more comprehensive DDoS mitigation strategy.

5.4 Install a web application firewall

A web application firewall (WAF) is a defence tool used to mitigate application layer DDoS attacks. It serves as a reverse proxy and creates a shield between the internet and your applications. It helps security experts identify any malicious traffic attempting to disrupt your services. A WAF allows you to exercise control over incoming traffic, permitting or denying access based on a predefined set of security rules. You can start with a basic set of rules and fine-tune them as you detect suspicious patterns associated with DDoS attacks.

5.5 Ensure continuous monitoring of network traffic

Continuous monitoring (CM) and real-time analysis of network traffic offers several benefits for identifying and mitigating potential DDoS attacks. Implementing intrusion detection systems (IDS) and intrusion prevention systems (IPS) for continuous monitoring of network traffic is effective in recognizing and blocking suspicious DDoS related traffic patterns. Leveraging these traffic analysis tools enables early detection of DDoS attacks, allowing for quick response before attacks escalate. Monitoring helps create a baseline of normal activity on a network or computer systems. This baseline should encompass both average and high-traffic days. It also helps in understanding normal network activity and traffic patterns, making it easier to differentiate between legitimate and malicious traffic and to identify unusual or suspicious activities. Around-the-clock monitoring will also allow for detection of an impending attack even during non-business hours and weekends.

5.6 Implement anycast network diffusion

Unicast routing, widely employed in network communication for its simplicity and versatility, serves various applications such as web browsing, email, and file transfers. In the unicast model, each network node or device is assigned a unique IP address, facilitating direct and efficient communication across the network. However, despite its simplicity, unicast is not resilient to DDoS attacks. As traffic is directed straight to a specific data centre, a DDoS attack has the potential to overwhelm the location or its surrounding infrastructure with excessive traffic. This surge can result in a denial-of-service situation, making it difficult to fulfill legitimate requests.

Unlike unicast routing, anycast network diffusion is more resilient due to its unique routing and addressing characteristics. Anycast disperses incoming traffic across a network of servers distributed in various locations, using the same IP address. This method expands the network's coverage, preventing any one location from becoming overwhelmed with malicious requests. When an address is sent an extraordinary amount of traffic, such as during a DDoS attack, traffic is automatically rerouted to the nearest available network location, thereby minimizing the impact on the primary infrastructure.

Anycast routing enhances network resilience, making attacks more manageable and reducing their potential for disruption, therefore ensuring uninterrupted service availability. A widespread network configuration makes it challenging for threat actors to execute DDoS attack, as it demands significant resources to send malicious traffic through a botnet effectively.

5.7 Conduct a risk assessment

A risk assessment will allow you to assess your organization's susceptibility to DDoS attacks. You should conduct regular risk assessments and audits on your network infrastructure to identify vulnerabilities. Although it's impossible to entirely prevent a DDoS attack, having a comprehensive understanding of your organization's hardware and software assets, including their strengths and weaknesses, is crucial to ensure adequate protection. Identifying the most vulnerable areas within your network is essential for determining the most effective strategy to mitigate the impact of a DDoS attack.

By conducting a risk assessment, you will:

- Identify critical assets to your organization and their importance to ensure ongoing operations.
- Analyze and evaluate potential threats that are relevant to your organization's business operation.
- Identify your organization's network vulnerabilities including weak points that threat actors might exploit and evaluate the impact and likelihood of the DDoS attack based on historical data, threat intelligence, and industry trends.
- Identify the different pathways that threat actors might use to initiate a DDoS attack, including methods like UDP flooding, SYN flooding, or HTTP flooding.
- Prioritize the identified risks by considering factors such as the likelihood of an attack taking place, the potential consequences of the attack, and the probability of both detecting and mitigating the attack.

5.8 Develop a DDoS attack response plan

To effectively prepare for a DDoS attack, it's crucial to have a well-structured response plan in place. This plan should include clear steps to help identify, mitigate, and recover from the attack. Your plan should also aim to minimize the impact on your organization and ensure uninterrupted or minimal downtime to your business operations.

Within this plan, the following components should be considered:

- Clearly outline and document the roles and responsibilities of all team members that will respond to a DDoS attack, including internal stakeholders, organizational leaders, and network administrators, as well as any involved service providers.
- Develop a comprehensive checklist that defines the processes and actionable items required during a DDoS attack. Specify the necessary tools and resources that will be needed and identify the individuals to be contacted.
- Establish a robust communication plan that outlines a predefined chain of communication to be followed in the event of a DDoS attack.
- Regularly conduct incident response exercises and ensure that your DDoS response plan is an integral part of your organization's overall disaster recovery strategy and business continuity plan.

5.9 Engage with a DDoS protection service provider

If your organization has limited resources to manage cyber security, you may want to consider engaging with third party entities to enhance your defence against cyber threats. They can offer various defence and protection services including DDoS scrubbing which can help protect your Internet traffic from DDoS attack. DDoS scrubbing involves filtering incoming traffic to identify and discard malicious data, allowing only legitimate traffic to reach the targeted network. This will allow you to maintain online presence during attacks without losing service.

Most ISPs and CSPs offer some level of protection against DDoS attacks. You should learn of the protective measures they provide and review the service agreement to identify any potential limitations in their coverage.

Using cloud-based DDoS mitigation solutions can also offer many benefits. These include dedicated staff to ensure quicker response time in the event of an attack and high network bandwidth which makes them more resilient against volume-based DDoS attacks. These solutions can also provide automated replication or backup options, allowing you to run your services without disrupting your users.

Should you require an even more robust DDoS protection solution, consider contacting an MSP to explore solutions tailored to your organization's needs to safeguard against DDoS attacks. These services are adept at actively monitoring your network traffic, detecting any signs of an attack, identifying its origin, and implementing measures to redirect harmful traffic away from your network.

Engaging with an MSP for DDoS protection offers numerous advantages. MSPs, specialized in cyber security, provide expertise, advanced technologies, and 24/7 monitoring for early threat detection. They deploy quick responses to mitigate attacks and scale services based on network needs. MSPs continuously update systems to stay ahead of emerging threats, providing a strategic and efficient approach to safeguarding online services. By entrusting DDoS protection to an MSP, your internal IT team can focus on core business operations, rather than constantly monitoring and responding to potential cyber threats.

6 Steps to follow after a DDoS attack

Dealing with the aftermath of a DDoS attack is an important step in enhancing your organization's resilience. After the attack is over, it's essential to evaluate its impact, reassess your defence strategy, and improve your overall preparedness for potential future incidents. Here are a few recommended key steps to complete this process.

- Analyze the attack post incident by identifying:
  - What assets and what part of the network were targeted?
  - What DDoS attack method was used?
  - How long did the attack last?
- Keep monitoring other network assets for other unusual or suspicious activity, as this might signal the possibility of a subsequent attack.
  - Assess the magnitude of the damage to understand its impact on your organization and identify the resources needed for future preventative actions. Key questions to consider include:
  - Which services were affected, to what degree, and for how long?
  - What were the financial losses incurred?
  - Did the attack harm your organization's reputation or lead to customer complaints?
  - Were there noticeable impacts on users due to the attack?
- Verify whether your third-party DDoS mitigation service provider has fulfilled their service level agreement (SLA) obligations as expected if you are currently using their services.
- Maintain transparency and effective communication by informing all stakeholders, including employees and customers, about the attack, its impact, and the mitigation steps being taken. Provide consistent updates on the recovery status and anticipated timelines to ensure everyone remains adequately informed. Continue to communicate about additional security measures being implemented to strengthen defences and prevent future attacks as this will demonstrate your organization's dedication to protecting the interests of your stakeholders.
- Identify ways to upgrade your DDoS defence solution. This entails assessing and reinforcing your DDoS protection strategy plan by identifying the root causes and vulnerabilities exposed during the attack. You should explore solutions to bolster your defences at both network and application levels. If you need an extra layer of protection due to limited in-house resources, consider exploring cloud-based DDoS mitigation options or using DDoS protection services from a third-party vendor. Additionally, it's crucial to routinely conduct vulnerability assessment and penetration testing to ensure the effectiveness of your defence solution.

7 Summary

In the landscape of cyber security, DDoS attacks represent a persistent and growing threat, orchestrated by various actors with malicious intent. These attacks aim to disrupt online services by overwhelming them with malicious internet traffic, potentially causing harm to organizations. DDoS attacks come in different forms, including volumetric attacks that saturate network bandwidth, protocol attacks that exploit vulnerabilities in data transfer protocols, and application layer attacks that target application weaknesses.

It is crucial for your organization to understand the potential effects of DDoS attacks, which range from revealing existing network weaknesses to financial setbacks and reputational damage. This understanding can help in the implementation of effective defence strategies to protect your digital infrastructure. These strategies should be regularly updated to address evolving threats and changes in network configurations. Assessing the aftermath of a DDoS attack enables a reassessment and improvement of defence strategies, ultimately enhancing preparedness for potential future incidents.

8 Supporting content

▶ 8.1 Supporting content

▶ 8.2 Glossary

8.3 References

1 Canadian Centre for Cyber Security. The National Cyber Threat Assessment 2023-2024, October 28, 2022.

2 Canadian Centre for Cyber Security. Protecting your organization against denial of service attacks - ITSAP.80.100, July 2022.

3 Cybersecurity and Infrastructure Security Agency. CISA’s DDoS Quick Guide (PDF), October 2020.

4 Canadian Centre for Cyber Security. How updates secure your device - ITSAP.10.096, March 2021.

5 Canadian Centre for Cyber Security. Secure your accounts and devices with multi-factor authentication - ITSAP.30.030 , June 2022.

6 Canadian Centre for Cyber Security. Spotting malicious email messages - ITSAP.00.100 , April 2022.

7 Canadian Centre for Cyber Security.Protect your organization from malware - ITSAP.00.057, July 2022.

8 Canadian Centre for Cyber Security. Virtual private networks - ITSAP.80.101, October 2019.

9 Canadian Centre for Cyber Security. Tips for backing up your information (ITSAP.40.002), October 2020.

Date modified: 2024-02-23

Government of Canada

All contacts
Departments and agencies
About government

Jobs
Immigration and citizenship
Travel and tourism
Business
Benefits
Health
Taxes
Environment and natural resources
National security and defence
Culture, history and sport
Policing, justice and emergencies
Transport and infrastructure
Canada and the world
Money and finance
Science and innovation
Indigenous peoples
Veterans and military
Youth

Social media • Mobile applications • About Canada.ca • Terms and conditions • Privacy

Canada